UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,188	04/20/2007	Glenn Mansfield Keeni	8075-1100	6594

466 7590 07/06/2010
YOUNG & THOMPSON
209 Madison Street
Suite 500
Alexandria, VA 22314

EXAMINER	
VICTORIA, NARCISO F	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
07/06/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DocketingDept@young-thompson.com

Office Action Summary	**Application No.** 10/588,188	**Applicant(s)** KEENI, GLENN MANSFIELD	
	Examiner NARCISO VICTORIA	**Art Unit** 2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 April 2007* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *8/02/2006*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the Application filed April 20, 2007.

2. Claims 10-26 have been examined and are pending. Applicant filed preliminary amendment cancelling originally filed claims 1-9, adding new claims 10-26.

Information Disclosure Statement

3. The Information Disclosure Statement (IDS) submitted on August 2, 2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the IDS statement is being considered by the Examiner.

Claim Objections

4. Claim 10 is objected to because of the following informalities: on line 8, the phrase “either of” needs to be changed to -- one of -- because the claim language provides more than two alternative conditions. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. § 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 13-14 and 24-25 are rejected under 35 U.S.C. § 102(e) as being anticipated by Chesla et al. (US 2004/0250124; hereinafter Chesla).

As per claim 13, Chesla discloses a network attack detection system, characterized in that it is judged that an illegal attack has taken place by observing the values of the packet header fields **(see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields to detect an attack)**, and when the number of distinct values seen in a combination of two or more header fields exceeds a pre-specified threshold value within a pre-specified time, it is judged that an attack is in progress **(see at least Para. [0033]: as part of detecting an attack, occurrences of at least one parameter among a plurality of parameters of packet headers are counted within a certain period of time and compared against a threshold value)**.

As per claim 14, Chesla discloses the network attack detection system according to claim 13, characterized in that judgment is made that an attack is in progress, if the Time to Live (TTL) value in the header of the packet does not lie in the range of the values seen beforehand for the source address in the header of the packet **(see at least Para. [0045]: one of the header fields that is monitored is time-to-live (TTL) when detecting an attack)**.

As per claim 24, Chesla discloses a method of detecting a network attack, comprising the step of:

observing values of packet header fields (**see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields to detect an attack**) and upon observing that a number of distinct values seen in a combination of two or more header fields exceeds a pre-specified threshold value within a pre-specified time, judging that an unauthorized attack is in progress (**see at least Para. [0033]: as part of detecting an attack, occurrences of at least one parameter among a plurality of parameters of packet headers are counted within a certain period of time and compared against a threshold value**).

As per claim 25, Chesla discloses the method of claim 24, wherein, observing a Time To Live value in the packet header and judging the unauthorized attack is in progress upon the observed Time To Live value being outside a range of the values seen beforehand for the source address in the packet header (**see at least Para. [0025-0026]; [0045]: for example, as part of measuring a property of a traffic entering the network and applying a fuzzy logic algorithm to detect an attack; packet header fields that are monitored include time-to-live (TTL), source IP address, packet size, and so on**).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. § 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 10-12, 15-17 and 20-23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chesla in view of Chao et al. (US 7,526,807; hereinafter Chao).

As per claim 10, Chesla discloses a network attack detection system, characterized in that a header of packet in transmission is examined and the values of one or more pre-specified fields in the packet header are observed (**see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields to detect an attack**), and in case the number of distinct values observed in the pre-specified fields reaches a pre-specified threshold within a pre-specified time interval, it is judged that an unauthorized attack is in progress (**see at least Para. [0033]: as part of detecting an attack, occurrences of at least one parameter among a plurality of parameters of packet headers are counted within a certain period of time and compared against a threshold value**).

Chesla does not explicitly disclose:

"and this judgment is carried out based on either of the following conditions:

(a) N(t) is the number of distinct values of the field observed within a pre-specified time interval from time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1 and if the ratio of N(t) to $N(t_1)$ is greater than, or equal to, some pre-specified threshold k_1, that is, if $N(t)/ N(t_1) > k_1$, the system will judge that an attack is in progress;

(b) P(t) is the number of packets in transmission within the pre-specified time interval from some time t, and if the ratio of the number of N(t) to P(t) is greater than, or equal to, some pre-specified threshold k_2, that is, $N(t)/P(t) > k_2$, the system will judge that an attack is in progress (see at l;

(c) $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from some time t_1, and if the ratio of the coefficient computed in (b) above for the time t to that computed for the time t_1, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\}$, is greater than, or equal to, some pre-specified threshold k_3, that is, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} > k_3$, the system will judge that an attack is under progress;

(d) T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t, and if the ratio N(t) to T(t) is greater than, or equal to, some pre-specified threshold k4, that is, $N(t)/T(t) > k_4$, the system will judge that an attack is in progress.

However, Chao discloses, in one embodiment, DCS 108 performing aggregation function 222 by comparing measured attribute values to nominal attribute values, wherein if the measured attribute value exceeds a predetermined threshold, DCS 108 may conclude that the packets are suspect, as in part of an attack (**see at least Figure 5 and Col. 9, lines 30-38: as stated by Chao's disclosure, one skilled in the art would appreciate that various thresholds and combinations thereof may be used to determine whether packets are suspect).**

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao to meet the preceding limitations. The motivation is to provide a distributed, adaptive Internet

Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 11, Chesla in view of Chao discloses the network attack detection system according to claim 10, characterized in that arbitrary combinations of two or more header fields are allowed, and the number of distinct values observed for the resultant composite field is used to compute the coefficient which is compared against the threshold (**see at least Chesla: Para. [0025-0026]: for example, as part of measuring a property of a traffic entering the network and applying a fuzzy logic algorithm to detect an attack**).

As per claim 12, Chesla in view of Chao discloses the network attach detection system according to claim 10, characterized in that it is inferred that an illegal attack is underway when the Time To Live (TTL) value in the header field of a packet does not lie in the range of the values seen beforehand for the source address in the header of packets (**see at least Chesla: Para. [0045]: one of the header fields that is monitored is time-to-live (TTL) when detecting an attack**).

As per claim 15, Chesla in view of Chao discloses the network attack tracking system according to claim 10.

Chesla does not explicitly disclose the system as being:

"characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 16, Chesla in view of Chao discloses the network attack tracking system according to claim 11.

Chesla does not explicitly disclose the system as being:

"characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 17, Chesla in view of Chao discloses the network attack tracking system according to claim 12.

Chesla does not explicitly disclose the system as being:

"characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 20, Chesla discloses a method of detecting a network attack, comprising the steps of:

examining a pre-specified field in a header of a packet in transmission for distinct values (**see at least Para. [0023], lines 5-8: performing statistical analysis on one or more packet header fields to detect an attack**); and

determining that an unauthorized attack is in progress based on an observed number of distinct values in the examined pre-specified header field reaching a pre-specified threshold within a pre-specified time interval (**see at least Para. [0033]: as part of detecting an attack, occurrences of at least one parameter among a plurality of parameters of packet headers are counted within a certain period of time and compared against a threshold value**).

Chesla does not explicitly disclose:

"wherein, the determination includes that at least one of the following conditions is satisfied

(a) N(t) is the number of the distinct values of the field observed within the pre-specified time interval from some time t, $N(t_1)$ is the number of distinct values of the field observed within the pre-specified time interval from some time t_1 and the ratio of N(t) to $N(t_1)$ is greater than, or equal to, a pre-specified threshold k_1, that is $N(t)/N(t_1) > k_1$,

(b) P(t) is the number of packets in transmission within the pre-specified time interval from some time t, and the ratio of N(t) to P(t) is greater than, or equal to, some pre- specified threshold k_2, that is, $N(t)/P(t) > k_2$,

(c) $P(t_1)$ is the number of packets in transmission within the pre-specified time interval from the time t_1, and the ratio of the coefficient computed in (b) above for the time t to that computed for the time t_1, $\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\}$, is greater than, or equal to, some pre-specified threshold k_3, that is, $\{N (t) /m (t) \} / \{N(t_1)/P(t_1)\} > k_3$, and

(d) T(t) is the number of octets or bits in the packets in transmission within the pre-specified time interval from some time t, and the ratio N(t) to T(t) is greater than, or equal to, some pre-specified threshold k4, that is, $N(t)/T(t) > k_4$."

However, Chao discloses, in one embodiment, DCS 108 performing aggregation function 222 by comparing measured attribute values to nominal attribute values, wherein if the measured attribute value exceeds a predetermined threshold, DCS 108 may conclude that the packets are suspect, as in part of an attack **(see at least Figure 5 and Col. 9, lines 30-38: as stated by Chao's disclosure, one skilled in the art would appreciate that various thresholds and combinations thereof may be used to determine whether packets are suspect)**.

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao to meet the preceding limitations. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 21, Chesla in view of Chao discloses the method of claim 20, wherein, said examining step examines a resultant composite field comprised of arbitrary combinations of two or more of header fields, and the number of distinct values observed for the resultant composite field is used to compute the coefficient which is compared against the threshold **(see at least Chesla: Para. [0025-0026]: for example, as part of measuring a property of a traffic entering the network and applying a fuzzy logic algorithm to detect an attack)**.

As per claim 22, Chesla in view of Chao discloses the method of claim 20, comprising the further steps of: from an examined packet, inferring that the unauthorized attack is underway when a Time To Live (TTL) value in the pre-specified field of the examined packet is outside a range of the values seen beforehand for the source address in the header of the examined packet, and after determining that the source address in the header of the examined packet is legitimate, detecting the unauthorized attack based on whether the Time To Live value is within a pre- specified range of the expected Time To Live value for the source address **(see at least Chesla: Para. [0025-0026]; [0045]: for example, as part of measuring a property of a traffic entering the network and applying a fuzzy logic algorithm to detect an attack; packet header fields that are monitored include time-to-live (TTL), source IP address, packet size, and so on)**.

As per claim 23, Chesla in view of Chao discloses the method of claim 20.

Chesla does not explicitly disclose the method as being:

“characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet.”

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao such that the method as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

9. Claims 18-19 and 26 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Chesla as applied to claims 13, 14 and 24 above, and further in view of Chao.

As per claim 18, Chesla discloses the network attack tracking system according to claim 13.

Chesla does not explicitly disclose the system as being:

"characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 19, Chesla discloses the network attack tracking system according to claim 14.

Chesla does not explicitly disclose the system as being:

"characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet."

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack (**see at least Fig. 1 and Col. 3, lines 56-67**).

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao such that the system as being characterized in that a source of the unauthorized attack is searched by setting these systems at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

As per claim 26, Chesla discloses the method of claim 24.

Chesla does not explicitly disclose:

"wherein, said observing step is performed at various places on the Internet. "

However, Chao discloses denial-of-service control servers that are distributed in a given network to form a system configured to protect against DDoS attack **(see at least Fig. 1 and Col. 3, lines 56-67)**.

Therefore it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Chesla and incorporate Chao such that said observing step is performed at various places on the Internet. The motivation is to provide a distributed, adaptive Internet Protocol (IP) filtering system and technique to detect and block packets involved in a DDoS attack (**Chao: Col. 2, lines 57-60**).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure:

Lau et al. (US 2004/0062199) - this reference discloses apparatus and method for an overload control procedure against denial of service attack.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NARCISO VICTORIA whose telephone number is (571)270-7904. The examiner can normally be reached on Monday to Friday 8:00am - 4:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/NV/

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438